

Electronic Fences or Free-Range Students:
Should Schools Use Internet Filtering Software?

David Pownell
016D Bluemont Hall
1100 Mid-Campus Drive
College of Education
Kansas State University
Manhattan KS 66506-5318
Voice (785) 532-5886
FAX (785) 532-73.04
dwp4231@ksu.edu
<http://www-personal.ksu.edu/~dwp4231/>

Gerald D. Bailey
303 Bluemont Hall
1100 Mid-Campus Drive
College of Education
Kansas State University
Manhattan KS 66506-5318
Voice (785) 532-5847
FAX (785) 532-7304
jbailey@ksu.edu
<http://www.educ.ksu.edu/go/bailey>

Electronic Fences or Free-Range Students:

Should Schools Use Internet Filtering Software?

Almost everyone has seen the movie “Titanic” and has been captivated by the story of human drama and adventure. Children become fascinated and want to find out more. Teachers can use this engaging topic to teach across content areas and truly use integrated learning. What better way to find information than to log on to the Internet? Searching for the term “Titanic” on the Internet will reveal a myriad of sites about the ship, but you may also find links to pornographic sites. While pornography is still only a small part of the Internet, it is increasing. Indeed, online sex was a \$925 million business in 1996 (Rose, 1997). This is a frustrating situation for educators who realize the great potential of the Internet as a teaching and learning environment yet have to deal with information that is not appropriate for students.

There is little argument that students **should not** be exposed to some types of information such as pornography, hate, slander and violence. Controls are in place in most areas of life to keep children safe and out of trouble. We buckle them in cars, rate their movies, and make them wear bicycle helmets. They are dependent on adults for taking some control of their environment. Katz (1996) noted that children need to have clear boundaries and occasional discipline in the digital age. These boundaries should extend in age-appropriate ways to the Internet, and many people believe that filtering software is a good way to protect children from online harm.

Stross (1997) suggested that the “filtering” of information has been going on for a long time. Pornography has been around for many years, and up until now, there has been an informal network of censors which included bookshop owners, newsstand proprietors, and librarians. In the past, the printing of materials also added to this system. Printing costs a good deal of money and materials were difficult to distribute. For these reasons, there was considerable control over what adults and children were able to access.

The Internet, however, is changing the way we think about and access all types of information. The unofficial filters no longer work in the new medium. Anyone can put any information on the web with only a small amount of money and knowledge. Because of this, there is no “sifting” of information—everything is always available to everyone. At this time, there is no control over the content of the Internet and with the defeat of the Communications Decency Act in 1997, there appears to be no final decision in sight.

Proponents of filtering software, such as New York University Professor Irving Kristol, feel that filters protect children from harmful information. He stated that “...if you believe that no one has ever been corrupted by a book, then you must also believe that no one has been improved by a book” (Kristol, 1995, ¶. 3). His argument is that information can and does change the way a person thinks and believes. Minnesota State Representative Charlie Weaver (R-Anoka) pointed out that “[i]f you can't have the stuff in your bookstore or in the library, then you shouldn't be able to have access to it on the Internet” (Qualey, 1997, ¶. 2).

Opponents of filters claim that they are a form of censorship and infringe on individuals' constitutional rights to information. There are also concerns about what messages we are sending to children when we filter the Internet. Filtering systems tend to incorporate value judgments about the content which is being blocked (Weinberg, 1997). This tends to divide information into “good” and “bad,” and it is unclear as to who will control it. With these arguments in mind, educators need to strike a thoughtful balance between exposure to content and the protection of students.

Fear is a major factor in the decision to use filters. Parents and educators have a fear for the safety and well-being of students. “Libraries [or schools] are not as safe a place as they used to be,” pointed out Sandi Zappa of the group known as K.I.D.S. (Keep Internet Decent and Safe). (Taaffe, 1997, ¶. 4). This fear of child safety is not

unfounded. There have been cases where children met people on the Internet and came to physical harm after meeting them in person. Conversely, Magid (1998) believes that there are far more dangerous and immediate threats to children in the physical world such as molestation by relatives, malnutrition, neglect, and insufficient health care. He downplays the idea of a “real” threat from the Internet.

There is also a fear over the loss of control of what information students can access and the ways they interact with it. Schools have always been in the business of regulating student behavior and controlling what materials students have access to (Schofield, 1994). This power has been used by schools to promote and reinforce local values and agendas. Connecting students to the Internet empowers children and that “terrifies a lot of people” (Huffstutter, 1998, p. D1). Students will now be able to experience new ideas that they did not have access to before. They are able to make connections to people that would not have been possible before the creation of Internet. As Katz (1996, p. 122) emphasized, the “kids are moving out from under our pious control, finding one another via the great hive that is the Net.”

Students are informal and unwitting ambassadors for schools. They are expected to act in “proper” ways in public settings, but the fear is that students will act in unfavorable ways online which educators cannot control. Schools believe that large numbers of people around the globe may see students acting in ways not representative of their school. Students can create web sites that mock and satirize their schools and teachers (Schofield, 1994). An example of this can be seen in a recent news story about a student who’s web site contained degrading remarks about a teacher. In the case, the courts determined that the school could not take any action because the incident was not connected to the school. In a basic way, the content of this Website is little different than students degrading teachers on paper or walls, but because of the speed and extensiveness of the Internet, the impact is far greater (“Web-site,” 1998).

These fears have convinced people that the Internet needs control and software filtering is a good way to do it. Most of the time, however, little thought is given to who controls the way that filters work and what the agendas are of the filtering companies. It is a complicated issue with many underlying arguments. As we will see, the federal and state governments are attempting to enact legislation to force schools into using filtering software while the software companies are trying to sell products that give an appearance of protecting children. Schools are caught in the middle trying to both protect children and give them a good education. Anyone who has watched with mixed emotions as his or her young child anxiously climbs the ladder of a large slippery slide knows the feeling. We want students to grow and develop while still being safe.

The Communications Decency Act was an attempt by the federal government to regulate what is put on the web. The Communications Decency Act was declared unconstitutional by the Supreme Court in 1997 ("Latest news," 1998). In response to the defeat, John McCain (R.-AZ), along with cosponsors Fritz Hollings (D.-SC), Dan Coats (R.-IN), Patty Murray (D.-WA), and Daniel Inouye (D.-HI), have introduced the Internet School Filtering Act (S. 1619). This bill will require schools and libraries to use filtering software to get federal money from the universal service fund (Harris, 1998). Schools fear that they will not get needed equipment if they do not install filters. Maury Lane, spokesman for Senator Ernest F. Hollings (D-S.C.) stated that "[i]f you want the money, you play by our rules. This is a way for the government to make sure schools are doing their job" (Huffstutter, 1998, p. D1). Although the bill will allow schools to choose which software they use, it is still a coercive and controversial move by the United States government.

Some state governments are beginning to mandate filtering in public schools. State Representative Charlie Weaver (R-Anoka) and Lt. Governor Joanne Benson of Minnesota have introduced a state bill which would require schools to use filtering

software and will cost the state \$57 million. The bill states only that filtering software be used, but does not specify the kind. This decision is left up to individual schools districts and schools. Even though Internet filtering would be state mandated, Weaver believes that “restraint [is] best exercised not by the government, but by corporations such as Net Nanny, CYBERSitter, Surf Watch and Cyber Patrol” (Qualey, 1997, ¶. 4).

Software companies who make the filters are in a position to wield great control as to what is and is not blocked. Most of them use “predetermined” blocking which uses databases of sites to be blocked (Kubota, 1997). Unfortunately for schools, most companies keep their lists of sites secret. McCullagh (1998, ¶. 5) noted that “[w]ith the exception of Net Nanny, every other censorware manufacturer treats its blacklist of thousands of forbidden sites as a trade secret and refuses to divulge its contents.”

Filtering software companies do give the general criteria for what constitutes blocking sites, but the actual sites are not given. CYBERSitter lists eighteen criteria which it uses to determine if a site will be blocked or not (“CYBERSitter”). Katz (1996, p. 169) argues that “[s]ome of these programs have thousands of potentially forbidden categories, going far beyond sex and violence.” Many of the filtering packages block legitimate topics such as feminism, pregnancy, fat-acceptance, guns, prison and penal institutions, and even sites criticizing blockers and censorship (Weinberg, 1997). Each company makes subjective decisions as to what sites should be blocked and believe they are acting with their customers interests in mind. Net Shepard uses a database of web sites rated by its users. People then “rely on the subjective ratings of unknown users confined to extremely broad categories” (Kubota, 1997, p. 698). This “mindless, comparison-based blocking of information” does not take into account the context of the information and suitable material may inadvertently be blocked. As a result, this act allows a potential for too broad a concept of protection. The filtering software also makes no distinction of what is appropriate for different aged students (Huffstutter, 1998). It is a “one-size fits all” proposition with schools naturally choosing protection

for the lowest common denominator.

Rating Internet sites using the Platform for Internet Content Selection (PICS) standard is another type of filtering. This format relies on site administrators to rate their own sites to a set of standard criteria (Kubota, 1997). The filtering software would then check to see what the PICS level was before allowing access. As an example of the rating system for a site which has nudity, the administrator has to decide if the nudity is “artistic, erotic, pornographic, or explicit and crude” (Weinberg, 1997, ¶. 22). We can see how the judgments made about sites would be both biased and subjective. Using the PICS standards, filtering software then has the ability to substitute alternative lists of sites from other sources such as the PTA, *Consumer Reports*, or the Christian Coalition (Stross, 1997). Although this seems to be a good idea, it would shift the control away from the government or software companies into the hands of special interest groups which may be even more divisive.

Schools need to have control over their curriculum and decide for themselves what is appropriate or not. There is much diversity in America and topics that are appropriate in one school may not be in another. As Guevara (1998, p. 6) relates, “classroom teachers are the instructional filters.” This implies that teachers are the best judges of what is appropriate in any given situation. The ISTE and the Consortium for School Networking have also argued for local control.

The decision whether to filter Internet access should be based on local values, the educational philosophy of the institutions involved, the manner [in which] the Internet is integrated into the curriculum and the ages of the students involved as well as review of the costs and benefits of the various software options (Harris, 1998, p. 2).

Clearly it would be difficult for any generic software program to take into consideration all of the variables necessary to decide what content should and should not be accessed.

Although local control is important, fear of what students will see and do on the Internet is having an effect on policy. As Huffstutter (1998, D1) stated, many schools are “making policy decisions based on a community’s perception of a threat, rather than on one that has been documented.” The few incidents of students being physically hurt because of Internet access has swayed public pressure towards filtering. Educators are taking a cautious stance and as, Santa Ana (CA) Superintendent Al Mijares says, “it’s better for schools to err on the side of scholastic control than student freedom” (Huffstutter, D1).

An example of schools which have put great restrictions on Internet access is in Santa Ana, California. Students and employees alike are restricted, not only from obvious sites which contain pornography and hate, but also from sites associated with sports, finance, and entertainment. Bob Halford, a graphic arts teacher, asked “[w]hy is it my students can get to the Catholic Church’s site, but they can’t read stories in USA today?” (Huffstutter, 1998, D1). This is a frustrating situation for teachers who are trying to incorporate the Internet into their teaching. Although staff can get access to some blocked sites, they must first file a request with their school principal. The principal then reviews the site and, if he or she approves, sends the request to district offices. Administrators then take a look and make a final decision. The final decision about what is blocked is made by a few people. This restrictive policy is pitting educators’ desires to help make students Internet-savvy against the needs to block material which is not inappropriate (Huffstutter).

Schools are caught in the middle with regards to the legalities on the issues of Internet access and filtering. If they do not use filtering, then they could be endangering students by allowing unrestricted access to harmful material. Conversely, if they do use filters, they may be violating the First Amendment rights of students.

Using filtering software without knowing what sites are blocked and which are not, puts schools in the position of unintentionally censoring materials which are

constitutionally protected. Kubota (1997) noted that this is called “unconstitutional overbreadth” and could leave schools open to laws suits of infringements of students’ First Amendment rights. Filters may also increase liability by claiming that they can keep students out of objectionable sites when in fact there is no way to guarantee that (McKenzie, 1996). If students are able to access inappropriate materials while filters are in place, parents are able to make the argument that the schools have broken their trust. Filters are not one-hundred percent effective and schools should not believe that filters will keep them from legal problems.

Another problem with filters is that schools or special interest groups can covertly push their agendas while appearing to “protect students.” They can intentionally block certain sites which are constitutionally protected by setting a high “level” of filtering while claiming that they are blocked because of permissible goals (Kubota, 1997). An example would be a school which covertly blocks homosexual content by using the guise of blocking sexual themes “The true intent of the school, hidden behind the proscribed categories, would not be easily determinable” (Kubota, p. 716).

As we have seen, the issue of who determines what is and is not blocked with filters is complex and will not be resolved soon. But, is the issue really whether we should use filtering software, or is the critical question whether we are preparing our students to live in the digital world of the 21st century? Does using filtering software teach children to make responsible choices about how they perceive the world, or does it simply teach kids how to defy authority? Huffstutter (1998, D1) relates that “[i]f kids want to see something—entertainment, sports, porn, whatever—they’re going to figure out a way to circumnavigate the filter.”

Free-range surfing may sound like we are giving children complete freedom, but that is not the case. Huffstutter (1998, D1) states that “[c]hildren have a right to access the digital culture freely, as long as they can access it safely and responsibly.”

We do not simply let them loose without constraints. We need to have appropriate education for making good choices about the Internet. In the following statement Rheingold makes his case for student education.

The locus of control is going to have to be in [the students] heads and hearts, not in the laws or machines that make information so imperviously available. Before we let our kids loose on the Internet, they better have a solid moral grounding and some common sense (1994, ¶. 8).

These “electronic fences,” like physical fences, do not build trust between people. “We need to teach ourselves how to trust children to make rational judgments about their own safety” (Katz, 1996, p. 170). We need to empower our children to come and talk to us about things they find that are objectionable. “If our kids come across something that is undesirable, we want them to talk to us about it and not feel they have done something bad which needs to be kept secret” (Tapscott, 1998, 243). [Software blocking] “is the antithesis of trust [in] rational discourse between adults and children and more evidence of the growing need to protect children not from smut, but from adult abuses of power” (Katz, 1996, p. 169). Filtering is like reading children’s personal notes or listening in on telephone conversations. Children learn trust and responsibility by example. If adults are not trustful of children then children will learn to be mistrustful of adults and the world in general.

Internet Filtering and School Choices

There are four basic options available to schools (See Figure 1):

Option 1: Employ Minimal/Zero Filtering System and Use Comprehensive Curriculum/Educational Materials Dealing with Digital Conduct (e.g., slander, copyright, spamming, flaming, hate groups, pornographic materials).

Option 2: Use Filtering Software and Employ Minimal Educational Materials Dealing with Student Digital Conduct.

Option 3: Use Filtering Software and Employ No Curriculum/Educational

Materials Dealing with Student Digital Conduct.

Option 4: Use No Filtering and No Curriculum/Educational Materials Dealing with Student Digital Conduct.

All advantages, disadvantages, and implications of each option must be discussed thoroughly to arrive at the most appropriate decision. This discussion **can not** occur in a vacuum. In the final analysis, schools must view their options from a systems perspective since Internet filtering systems impact all other facets of technology integration. Technology leaders in the school district should approach this issue by using a four-step model:

1. Empower technology leaders to deal with the issue. This decision is not a single person (i.e., superintendent or principal) responsibility. A technology leadership committee should have the responsibility for considering what options should be considered and adopted (See Figure 1):

2. Empower the technology leadership committee build consensus as they consider which option is best suited for that school district.

Parents, community members, faculty, and students should be involved in determining the use of filtering software and/or creating curriculum materials related to digital conduct (e.g., units, lesson plans, digital conduct statements). Ultimately, that recommendation by the technology committee should be forwarded to the superintendent and board of education.

3. Establish a knowledge base concerning the options. Knowledge from experts and research must be at the center of the decision-making process. While discussions about filtering systems provoke emotional responses, technology leaders must create an environment of intelligent decision making. This includes inviting business and industry (who are facing similar decisions) to testify about employee behavior when on the Internet and their response. Benchmark your decision against the leaders in the field of technology--not just what other schools are

doing.

4. Empower the Technology Leadership Committee to evaluate and review the program/policy annually and report their recommendations to the board of education and other stakeholders in the community. The Internet filtering policy/program which is adopted should be monitored and evaluated for its effectiveness.

Conclusion

Obviously, the authors are not without their own conclusions. After countless hours of debate, site visitations, and research, we believe that *Option I: Employ Minimal/Zero Filtering System and Use Comprehensive Curriculum/Educational Materials Dealing with Digital Conduct (e.g., slander, copyright, spamming, flaming, hate groups, pornographic materials)* deserves the technology committee and stakeholders highest consideration in the decision making process. But whether you build an electronic fence or create free-range students on the Internet is a school-based decision--not ours.

It is our belief that schools need to prepare kids to live in the world, not just "protect" them from it. The rate of change has increased tremendously. Often, we are in a mind set of a world in which "it was good enough for us," but that world no longer exists (Katz, 1996, p. 123). Education and responsibility building needs to be foremost in our minds while censoring should only be used as a last resort with kids and the Internet.

Children are our future and as Jon Katz implores "[i]nstead of holding them back, we should be pushing them forward. Instead of shielding them, we should take them by the hands, guide them to the gates, and cheer them on" (Katz, 1996, p. 170). The great sociologist Emile Durkheim put it this way, " [w]hen mores are sufficient, laws are unnecessary. When mores are insufficient, laws are unenforceable" ("Lessons," 1996). Let's teach our children well.

References

- CYBERSitter Site Filtering Policies. [Online]. Available:
<http://www.solidoak.com/cybpol.htm>
- Guevara, L. (1998). Plain or filtered: Considering a filter program? Some notes from a high school classroom. Educom Review, 3(2), 4-6.
- Harris, L. (1998). Washington Notes. ISTE Update, 10(6), 1-3.
- Huffstutter, P. J. (1998, March 30). Censors and sensibility: Are some schools going too far in protecting kids from inappropriate Web sites? Los Angeles Times, p. D1.
- Katz, J. (1996). The rights of kids in the digital age. Wired, 4(7), 120-123, 166-170.
- Kristol, I. (1995). Pornography, obscenity, and the case for censorship. English Composition Board [Online]. Available: <http://www-personal.umich.edu/~wbutler/kristol.html>
- Kubota, G. (1997). Public school usage of Internet filtering software: Book banning reincarnated? Loyola entertainment law journal, 17, 687-731.
- Latest news: The struggle isn't over yet. (1998, March 30). Electronic Frontier Foundation [Online]. Available: <http://www.eff.org/blueribbon.html>
- Lessons in Leadership. (1996). Business Leader [Online], 2(4). Available:
<http://www.businessleader.com/blsep96/vision.html>
- Magid, L. J. (1998, January 6). Much ado about almost nothing. [Online]. Available: <http://www.larrysworld.com/articles/muchado.htm>
- McKenzie, J. (1996). A dozen reasons why schools should avoid filtering. From Now On [Online], 5(5). Available: <http://www.fromnowon.org/mar96/whynot.html>
- McCullagh, D. (1998). Lose it! Yahoo! Internet Daily Life [Online]. Available:
<http://www.zdnet.com/yil/content/mag/9803/blockdeclan.html>

Qualey, M. L. (1997). Bill: Babysit the 'Net. Channel 4000 [Online]. Available:
<http://www.wcco.com/news/stories/news-970206-111851.html>

Rheingold, H. (1994). Why censoring cyberspace is futile. The Well's Virtual Community Conference [Online]. Available:
<gopher://riceinfo.rice.edu:1170/00/More/Acceptable/rheingold>

Rose, F. (1997). Sex sells. Wired, 5(12), 218-224, 276-284

Schofield, J. (1994). Cyberspace superhighways: Access, ethics and control. Transcript of the John Marshall law school conference [Online]. Available:
<gopher://riceinfo.rice.edu:1170/00/More/Acceptable/k12trans>

Stross, R. E. (1997). The cyber vice squad. U.S. News & World Report, 122(10), 45-48.

Taaffe, L. (1997, August 6). How much access? Los Altos Town Crier [Online].
<http://www.losaltosonline.com/latc/arch/9732/CoverSto/cover/cover.html>

Tapscott, D. (1998). Growing up digital. New York: McGraw-Hill.

Web-site suspension earns student 30k. (1998, April 14). Wired News [Online].
Available: <http://www.wired.com/news/news/politics/story/11650.html>

Weinberg, J. (1997). Rating the net. [Online]. Available:
<http://www.msen.com/~weinberg/rating.htm>

II**Use Filtering Software & Minimal Education of Digital Conduct** (Curriculum, AUPs, etc.)**Advantages:**

- teaches some awareness for appropriate online behavior
- filters block some inappropriate material
- some legal protection

Disadvantages

- AUPs not really educating students
- filters give false sense of security
- difficulty accessing good sites
- high filter cost
- legal issues of censoring Constitutionally protected material--violate civil liberties
- legal issues for failure of filters
- software companies determine what is filtered, possible hidden agendas
- some inappropriate material accessed

Implications:

- some awareness of online responsibility
- continued search for best filtering system

I**Use Minimal/Zero Filtering & High-level Education of Digital Conduct** (Curriculum/Units on Digital Conduct)**Advantages:**

- teaches responsibility, accountability
- teaches children to live in an uncensored world (benefits/liabilities)
- prepares students for future
- no filter expense

Disadvantages

- need for developed curriculum/education materials
- need for teacher training
- adds to teaching load
- opposition from advocates of filters
- some inappropriate material accessed

Implications:

- high level of online responsibility
- continuous need for leader involvement
- need for regular program reevaluation
- need for community understanding and support

IV**Use No Filtering System & No Curriculum/Education of Digital Conduct****Advantages:**

- no filter expense
- no expense for teacher training

Disadvantages:

- no protection from inappropriate material
- students do not learn appropriate online behavior
- no faculty involvement
- some inappropriate material accessed

Implications:

- low level of online responsibility
- students are ill-prepared for world of work

III**Use Filtering Software & No Curriculum/Education of Digital Conduct****Advantages:**

- some protection
- may work for places where there is no supervision

Disadvantages

- students don't learn appropriate use
- high Internet filter cost
- difficulty accessing good sites
- filters give false sense of security
- legal issues of censoring Constitutionally protected material--violate civil liberties
- legal issues for failure of filters
- no leadership/community involvement
- software companies determine what is filtered, possible hidden agendas
- filters increase attention to inappropriate material
- some inappropriate material accessed

Implications:

- low level of online responsibility
- external control of student behavior/choices

Figure 1